Growing Pains, Risks as Internet and Social Media Proliferate

The rapid integration of digital technologies into everyday life continues to create new risks and challenges that many individuals and families frequently overlook or do not yet fully appreciate.

Take these two technological developments: Smartphones and the Internet of Things (IoT). While smartphone and mobile technology as a whole has put the Internet at the fingertips of a greater number of people worldwide, it also has allowed the development of millions of applications that collect and store large quantities of personal data that could easily fall into the wrong hands. Today's mobile users not only have to contend with the unsafe data collection of certain mobile apps, but they must also be on guard for hackers who have developed fraudulent versions of popular apps designed to steal personal data, such as credit card information.

The Internet of Things, where everyday objects have network connectivity, allowing them to send and receive data, is another example of an emerging security risk. As more devices become Internet-enabled – **24 billion by 2020, according to a recent estimate** – experts are finding that IoT devices often lack basic security measures such as proper encryption. For example, last year, security experts were able to remotely gain control of a moving Jeep Cherokee, raising questions about automakers' ability to secure connected cars.

While responding to some emerging technological risks requires a level of technical sophistication, other risks can simply be avoided or mitigated through diligence, education and proactive engagement with risk management specialists.

At USI Insurance Services, our team of Personal Risk Specialists advise individual clients and families on ways to better manage risks associated with the use of technology for communication, security and efficiency.

Following are a few specific examples:

Protecting Against Online Predators

The statistics on online predators are terrifying. According to the National Sex Offender Public Website:

- Approximately 1 in 7 (13-percent) youth Internet users received unwanted sexual solicitations
- 9-percent of youth Internet users had been exposed to distressing sexual material while online
- 15-percent of cell-owning teens (12–17 year-old) say they have received sexually suggestive nude/seminude images of someone they know via text.

Unfortunately, many experts believe these statistics will only worsen as more children gain access to a growing number of Internet-connected devices. It is estimated approximately **95 percent** of all Americans between **12 and 17 years old** are online and three in four teens access the internet on cell phones, tablets, and other mobile devices.

It is critical that parents and guardians monitor the activity of younger children in order to protect them from online predators. USI can assist parents with obtaining the appropriate monitoring tools.

Facing up to Cyber-bullying

Research by Cox Communications Inc., in partnership with the National Center for Missing & Exploited Children, found that 19-percent of teens have reported being victims of online bullying.

The study also shows the incidence of online harassment is higher (23-percent) among 16 and 17 year-olds, and that girls are more likely to be harassed or bullied than boys.

For both the victim and perpetrator, there can be severe financial consequences. The

costs may include counseling expenses, individually and for the family, as well as medical treatment for any injuries resulting from bullying. Legal expenses may also be incurred.

Carriers have begun to develop insurance protection for families due to injuries sustained from cyber-bullying. USI can help individuals obtain suitable liability coverage for such injuries, even if it is caused unintentionally via the internet or social media.

Recently, a child of a USI client reported experiencing online harassment by a classmate. Through the advice provided by USI, the parents began to actively monitor the child's online activity. As a result, the family avoided any serious consequences from the verbal abuse their son was receiving. The expenses related to counseling were minimal, but more importantly, the child was kept safe and avoided additional damage to his self-esteem, grades and overall well-being. The perpetrator also avoided serious legal issues and gained a better appreciation for the effects of cyber-bullying.

Exercising Constraint on Social Media

Social media allows individuals to share views and opinions on virtually any topic with a global audience.

For individuals who are unable to constrain their activities online, whether making inappropriate comments or sharing explicit photos, the potential impact to their reputation and finances could be significant. Risks include legal responsibility for libel, slander, loss of employment and income. In addition, transmitting photos or videos of others without consent can lead to criminal and civil action against the individual who transmitted the material.

USI's approach is to educate parents and children on social media etiquette and appropriate behavior, coupled with the use of software and active monitoring of activity on social media.

Securing Personally Identifying Information

In 2014, a new identity theft victim was reported in America every two seconds as identity thieves lifted a total of **$16 billion** from **12.7 million consumers**, according to a study by Javelin Strategy & Research.

While credit monitoring and protection systems are helping to catch and deter criminals, identity theft and fraud remain widespread, with hackers able to sell sensitive personal information for $9 to $40 per record. Driven by the high value of records on the black market, hackers continue to pursue vulnerabilities in technology, such as unsecured WiFi portals and mobile applications.

Among other things, USI advises clients and their families to not access financial institution websites from a public or unsecured WiFi portal. Other recommendations include:

- Close management of passwords for all financial accounts
- Never use names, dates of birth, current addresses or the word "password" for access to your accounts
- Individuals may purchase coverage through a homeowner's policy, or from credit card companies and other sources
- Any ID Theft coverage must include active monitoring of credit activity with immediate notice of suspicious or unknown requests for credit.

In a recent notable event, a financial advisor received an email alert from a credit card company about several attempts to charge $3,000 on a card. The advisor, who frequently monitors his assets, reached out to his bank and learned that $80,000 had been transferred from his valid account to five newly established fraudulent checking accounts.

Eventually this advisor, who had obtained a USI-negotiated ID theft coverage, was able to recover all the stolen funds. In addition, through the coverage, he was able to work with an advocate to restore his credit, including completing identity theft affidavits, notifying the Federal Trade Commission and IRS and reviewing current credit reports to identify every piece of fraud to dispute. This client avoided more than **$106,000** in potential out-of-pocket expenses as a result of the coverage.

These are only a few examples of how USI is helping individual clients manage Internet and social media-related risks, and keep themselves and their families safe. The USI approach encourages not only proactive engagement with risk management specialists but also constant education and information-sharing to stay abreast of this ever-changing risk.

To learn more about these and other solutions, contact your local USI personal risk specialist.